

Poster: Global Security Risk Classification Method for Cloud Migration of Industrial Internet Apps

Rajika Tandon
 Cybersecurity & Technology Risk
 GE Lighting, General Electric (GE)
 Cleveland, OH, USA
 rajika.tandon@ge.com

Corey T Jackson
 Cybersecurity & Technology Risk
 GE Lighting, General Electric (GE)
 Richmond, VA, USA
 corey.T.jackson@ge.com

I. INTRODUCTION

Organizations are looking to migrate their applications (apps) to the Cloud [1] for cost benefit, location independence, higher availability, and fault tolerance. Based upon severity of risks to the business posed by an application as per the criticality of data processed or stored by it, Security Risk Classification Level or Security Categorization [2] of an application is determined as low, medium, high, or crown jewel. Such risk classification helps in determining the security controls that needs to be built into the cloud so as to protect the apps of different risk levels appropriately. Best practice is to keep separate clouds (Virtual Private Clouds [3] or VPCs) with appropriate security controls built-in to handle required risk level of apps. Therefore, risk classification of apps is a very important step before migrating them to the appropriate VPCs.

Different nations may pose a challenge in risk classification depending upon laws governing specific industries, transfer/storage, and license limitations. Thus, making it more complicated for an international organization to appropriately classify security risk for its cloud-based application. As a huge global company, GE has designed a process that will classify an application into appropriate risk level/category based upon certain security risk flags, where such risk flags are representative of sensitive data or information (see table 1) that poses a security concern. This process also involves an application management tool to assist in classification.

II. OBJECTIVE

To assess the workflow of security risk classification of applications using the methodology designed by GE/GE Lighting (GEL) prior to cloud migration.

III. METHODS

Methodology utilized by GE/GEL to classify applications into different security risk buckets/levels is shown in table 1. There are 191 GEL's Industrial Internet [4] apps that reside in its data center. Security risk classification of all apps was performed earlier using basic classification model and was not verified. Moreover, some apps could then have been incorrectly classified or may required classification change later due to added functionalities over the course of time. Depending upon risk level of an app (low, medium/med, high), it has to be moved to the corresponding level of internal cloud or VPC (low, medium, high). Therefore, it is imperative that apps are correctly classified so as to migrate to appropriate

VPC. The new classification methodology identified fine-grained security flags/critical data than the basic classification model. This new methodology along with associated tool thus provided features to better identify risk associated with an app and appropriately classify its security risk level.





 Low Risk	 Medium Risk	 High Risk	 Crown Jewel
Loss or compromise of this system, or data processed or stored by this system could have:			System identified by executive leadership as Crown Jewel.
minimal negative impact to GE.	risks to privacy, reputation or operations. Includes data related to employee, contractor, consumer, customer, intellectual property -high/medium, SOX /non-SOX financial reporting, product quality, key security tools & process (physical & IT)	regulatory penalties, significant financial or competitive harm. Includes PII related to medical records, bank accounts, credit card, PCI data, SSN, Govt. IDs, and special data; intellectual property – business critical, Govt. classified & controlled unclassified, Govt. export control, non-public 3rd party contractual data	Includes mission-critical or business-critical capabilities, use cases, and assets

Table 1: Security risk classification of an app based upon data processed/stored

Total 54 Application Owners (App Owners or AOs) were identified to own the 191 apps. We re-calculated classification of each app based upon the currently marked security risk flag values by their AOs. Our findings show that 58 apps were incorrectly classified (see table 2). To ensure the correctness of security risk flags/classification of apps, all App Owners and Managers were notified with the business requirement and were provided 2 weeks deadline for classification/verification of their apps, along with the reference documents.

Previous Classification	Calculated risk classification		
	Low	Med	High
Low	-na-	11	1
Med	41	-na-	2
High	3	0	-na-

Table 2: Calculated risk classification levels of previously incorrectly classified apps

IV. RESULTS

Response of Application Owners to the notification to verify/update the risk classification of their applications, is summarized in table 3. Table 4 provides response of App Owners within deadline (2 weeks).

Response	App Owners (Total 54)	Response in 2 weeks	No. of Apps
Responded and completed classification	22	Total apps verified/ correctly classified	83 out of total 191
Responded but did not complete classification	8	Incorrectly classified apps that got corrected	23 out of 58 (see table 5)
No response in 2 weeks	24	Apps verified but no changes made	41
*94% AOs complied by 90 days		Apps with security flags update (same classification level)	14
		Apps verified with other info update such as Functional/ App Owner, etc. (same risk/flags)	4

Table 3: AOs' responsiveness Table 4: Summary of classification of apps

Also provided are: first response time by AOs to the notification received in fig. 1, data on AOs requiring help with classification in fig. 2, and time taken by AOs in completing verification/classification of their apps in fig. 3.

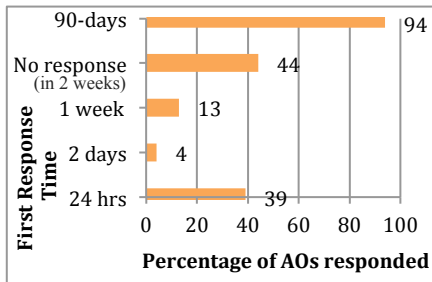


Fig. 1. Graph depicting response time of App Owners (AOs)

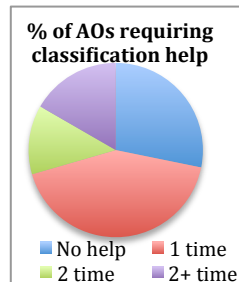


Fig 2: AOs (%) requiring help with classification

Top 4 challenges faced by the Security Team are:

- Limited security experience of AOs and the over-classification of security (flag/rank higher by default)
- Reaching some App Owners as they changed but not updated in database (containing details of each application)
- Limited security team manpower to meet individually with every App Owner to determine security risk
- Clarity in roles for contacting App Owners: Security vs. Technology team, Project Manager vs. Architect

Top 4 challenges faced by the Application Owners are:

- Limited security experience/knowledge
- Insufficient illustrative examples/explanation in the tool and understanding from reference documents could take time
- Limited time to complete
- Backups for App Owners/Managers to complete the classification in time if the later are unavailable.

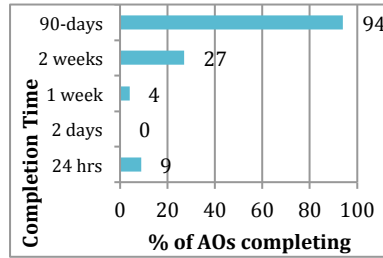


Fig. 3: Graph depicting time taken by App Owners (AO) to complete classification

Previous	Re-classified apps		
	Low	Med	High
Low	-na-	6	1
Med	14	-na-	0
High	3	0	-na-

Table 5: Previously incorrectly classified apps that got re-classified by App Owners as per our calculation

V. CONCLUSIONS

Our process helped in re-classification of 40% incorrectly classified Apps and a total of 44% apps got verified by the end of 2 weeks (deadline). By the end of 3 months, a total of 98% Apps were verified/complied with 94% of App Owners responding to the notification and complying.

To our knowledge this is the first study which has assessed the workflow and challenges of security risk classification for applications. Our experience showed that this methodology provided much thorough classification of security risk level due to all the possible security risk flags it considered. Modifications to the app management tool as outlined below may lead to further improvements:

- Providing more explanation of each security risk flag with illustrative examples.
- Automatic calculation of risk classification level based upon security risk flags selected.
- Periodic automated reminders to the App Owners to verify security entries of their applications.

Overall, the workflow provided better security awareness to the App Owners. However, more security training is required and pro-active measures need to be built in the app that can alert the App Owners to verify/update classification when any change is made to the app that may affect security.

ACKNOWLEDGMENT

The authors would like to thank John Hepp and Ken Soukup, employees at GEL, for helping with the process of finding applications with classification defects, and also the GE Corporate Security Team for their contribution in security risk classification and app management tool.

REFERENCES

- J. W. Rittinghouse, J. F. Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, 2009, pp. xxvi-xxvii.
- K. Stine, R. Kissel, W. C. Barker, J. Fahlsing, J. Gulick, "Guide for Mapping Types of Information and Information Systems to Security Categories", vol. 1, National Institute of Standards & Technology, 2008.
- T. Erl, Z. Mahmood, R. Puttini, "Cloud Computing: Concepts, Technology & Architecture", 1st ed., Prentice Hall, 2013, pp. 75-76.
- J. Bruner, "Industrial Internet", 1st ed., O'Reilly Media, 2013.